Cloud Storage Forensics: Amazon Cloud Drive on Ubuntu

Ming Sang Chang

Department of Information Management, Central Police University,
Taoyuan City, 33304, Taiwan (R.O.C.)

Abstract

Cloud storage services are increasingly used by consumers, business, and government. These services are fairly easy to obtain. Amazon Cloud Drive is a cloud-based storage that allows users to transfer files to and from multiple computers. This paper was undertaken to determine the data remnants on an Ubuntu computer. We focus on exploring the cloud activities of Amazon Cloud Drive and try to obtain evidences that may be left under these activities, and different Internet browsers. By determining the data remnants on client devices, we attempt to enhance the efficiency of the digital forensics and crime investigation.

Keywords: *Amazon Cloud Drive, Cloud Storage Forensics, Digital Forensics, Ubuntu.*

1. Introduction

Cloud computing is a model for enabling ubiquitous network access to a shared pool of configurable computing resources [1]. The users of cloud computing can alleviate big capital investments, replacing them with low cost and more flexible operational expenses, while taking advantage of its speed, agility, flexibility, infinite elasticity and more importantly mobility because services can be accessed anytime and anywhere [2]. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers [3].

According to a new forecast from International Data Corporation (IDC), public IT cloud services spending will grow to more than $149 billion in 2019 [4]. A study by Market Research Media found that the global cloud computing market is expected to grow at a compound annual growth rate of 30% reaching $270 billion by 2020 [5]. A recent study conducted by RightScale group on the adoption of cloud computing, concluded that 95 percent of organizations surveyed are running applications or experimenting with infrastructure-as-a-service in January 2016 [6]. It already has begun changing how IT delivers economic value to countries, cities, industries, and businesses. The availability of cloud storage services is becoming a popular option for consumers to store data.

Internet brings a lot of convenience for modern life, but also caused many emerging crime problems. Since the information technology and mobile networks developed, resulting in crime figures increase rapidly. The criminals may use cloud storage for criminal purpose. It adds to the challenge of digital evidence in cases under investigation. Cloud storage services can be used to store, access and distribute data via remote infrastructure in overseas jurisdictions to avoid the scrutiny of law enforcement agencies [7].

While criminals are scrutinized by law enforcement agencies, the Internet crimes are effectively suppressed. But it is still a security issue that can’t be ignored. For computer crime investigators, set up a systematic investigation procedure and confirm each of digital evidence to prove the offense is very important. It is important to have a strict methodology and set of procedures for executing digital forensic investigations and examinations. In addition, it is also important to have a contemporary understanding of the location and type of data remains left behind by cloud storage users on the devices they use to access their data [8].

The focus of this research is to discover whether there are any cloud storage data remnants on a client device. In this paper, we discuss the digital forensics, and conduct research into the data remnants of a user accessing Amazon Cloud Drive in a variety of ways, and also undertaking anti-forensics to hide the use of cloud storage on an Ubuntu PC. The rest of this paper is organized as follows. In section 2, we show the literature survey of existing related works. Methodology and research preparation is presented in section 3. Result and analysis is presented in section 4. Section 5 is a conclusion.

2. Related Works

Cloud computing provider provides their services according to different models; infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [9]. IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. In the software as a service (SaaS) model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications [10]. National Institute of Standards and Technology (NIST) also describe four deployment models for cloud services; Private cloud, Community cloud, Public cloud, and Hybrid cloud. Because of an increase in the use of computers and storage devices by criminals, forensic computer analysis is a recent discipline [11]. The Criminals can store illicit data on cloud storage. Cloud storage provides services which distance from the criminals. Hence, criminals can avoid the scrutiny of law enforcement and national security agencies.

McClain discusses Dropbox client software from a forensic perspective. He found Some data remnants on the machine of cloud end user. He concluded that registry changes, updated files, web cache, and deleted files recovery are the major remnants found on Windows 7 [12]. Chung did a research on forensic remnants of cloud storage on different operating systems. They present methods for collecting and analyzing evidence about a variety of the cloud storage services [13].

Jason discusses the digital artifacts left behind after an Amazon Cloud Drive has been accessed from a computer. Methods available to a forensic examiner that can be used to determine file transfers that occurred to and from an Amazon Cloud Drive on a windows 7 computer [14]. Darren Quick discusses data remnants on end user devices of using Dropbox. They want to determine the data remnants on a Windows 7 computer and an Apple iPhone 3G when users use different methods to store, upload, and access data in the cloud [15]. Darren Quick discusses data remnants on user machines of using Google Drive. They use a computer and an iPhone to access Google Drive. They want to discover the remnants left on client devices. After a user accesses Google Drive, They examine the benefits of using a proposed framework to guide an investigation when undertaking forensic analysis of a cloud computing environment [16]. Darren Quick also discusses data remnants on user machines of using Microsoft SkyDrive. They use a computer and an iPhone to access Microsoft SkyDrive [17]. S. Mehreen discusses the identification of data remnants of a user activities related to Dropbox usage on Windows 8. They focused on the cloud end user and aimed at finding the data remnants of cloud storage activity, specifically Dropbox on Windows 8 platform [18]. Zhu examines Skype, Viber, Mail, and Dropbox mobile cloud applications on Android and iPhone iOS mobile devices in depth as three scenarios. In relation to Dropbox, Zhu reported that filename and username information was able to be extracted in relation to Dropbox use [19]. Reese describes a process of using snapshots using EBS Boot volumes in Amazon cloud services where there is the ability to snapshot a system [20]. Clark examines picture Exif metadata remnants in Microsoft SkyDrive, Windows Azure, and Flickr, focusing on the information within pictures that are publicly shared [21].

All of the above mentioned research has been done on versions of Windows, iOS, and Android. Thus the cloud storage forensics on Ubuntu remains an area to be explored. We also find there are no researches have been done on Ubuntu. In this paper, we will discuss the identification of data remnants of a user activities related to Amazon Cloud Drive usage on Ubuntu.

3. Methodology and Research Preparation

This research focus on what data remnants after a user has accessed, up-loaded, and downloaded data from Amazon Cloud Drive. Our study uses different browsers to test it. There is no Amazon Cloud Drive client software to support Ubuntu OS and Microsoft Internet Explorer does not support Ubuntu either. We use the popular browsers include Mozilla Firefox, and Google Chrome. We use these browsers in our research to determine any differences in the ability to retrieve data remnants. We want to find username, password, files, and text within files. In addition, we also create circumstances to simulate a user running BleachBit to remove evidence of using Amazon Cloud Drive.

We make multiple scenarios to explore the use of Amazon Cloud Drive with a different browser. We create 10 Virtual Machines for each browser to replicate different circumstance of usage. According to the operation of Amazon Cloud Drive, we create five sub-experiment systems for each browser. They are Base, Access, Download, Upload, and BleachBit.

We use the base image files to compare the subsequent image files to determine the changes made. It is possible to observe the changes of registry files and file systems. We use VMware Workstation 10.0.0 to create virtual machine. For each browser scenario, a base image was created. We install Ubuntu 14.04.1 on a 20 GB virtual hard drive with 1 GB RAM. The Base-VM files were used as control media to determine the files created when user activity was undertaken in each scenario. All scenarios for Ubuntu are shown in table 1.

Table 1: All Virtual Machine Files

Browser VM	Mozilla Firefox	Google Chrome
Base-VM	UMF-Base	UGC-Base
Upload-VM	UMF-Upload	UGC-Upload
Access-VM	UMF-Access	UGC-Access
Download-VM	UMF-Download	UGC-Download
BleachBit-VM	UMF-BleachBit	UGC-BleachBit

We describe the details of our experiments as follows.

1. We install different browser software into separate Base-VMs. They are Mozilla Firefox (MF) v31.0, and Google Chrome (GC) v39.0.2171.
2. We make a copy of the Base-VM for each browser and Amazon Cloud Drive. These 8 VMs are labeled UMF-Access, UMF-Download, UMF-Upload, UMF-BleachBit, UGC-Access, UGC-Download, UGC-Upload, and UGC-BleachBit.
3. We use upload virtual machines to upload test files. These upload virtual machines are UMF-Upload, and UGC-Upload. The test files are uploaded to Amazon Cloud Storage. Then we delete test files from the virtual machines. After we open the test files from Amazon Cloud Storage, we close the browser, then shut down the system.
4. In these virtual machines, UMF-Access and UGC-Access, we use different browser to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we log out and close the browser, and shut down the system.
5. The download virtual machines are UMF-Download, and UGC-Download. We use different browser to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we download the test files on the desktop of virtual machines. We open the download files. Then we log out and close the browser, and shut down the system.
6. We use BleachBit 1.6 software to do anti-Forensics. These anti-Forensics virtual machines are UMF-BleachBit, and UGC-BleachBit. We do the same action as download virtual machines. Then the downloaded test files are deleted. We run BleachBit 1.6 software to clear temporary files, test files, and browsing history.

4. Result and Analysis

After all the experiments, we use Guidance EnCase v7.04 to analyze VMDK files of all virtual machines. This research is to determine the data remnants on an Ubuntu PC for the use of Amazon Cloud Storage. We try to find username, password, browser access, software access, and files stored within the account. We use keywords to search the data remnants. They include Amazon, account name (testforensic2014), account password (test123456789), test files (1.bmp, 1.jpg, 1.doc, 1.xls, 1.ppt), and the text within the test files (This is Microsoft word, This is Microsoft excel, This is Microsoft PowerPoint).

There are five different kind experiments to be discussed.

Base-VM

There are two Base-VM hard drives, such as UMF-Base, and UGC-Base. They have no data originally present relating to the sample test data and Amazon Cloud Storage files. We Analyze this two control Base-VM hard drives to confirm there was no data originally relating to Amazon Cloud Storage. The control VM's in this case have shown that data matches will occur, even when user activity in relation to Amazon Cloud Storage has not been undertaken.

Table 2: The remnants of Access-VMs

Keyword	Firefox	Google Chrome
Amazon	•\home\[username]\ .cache\mozilla\firefox\sellmnkv.default\Cache •\usr\lib\ •\usr\share\ •\Unallocated Clusters	•\home\[username]\ .cache\ google-chrome\Default\ •\usr\lib\ •\usr\share\ •\Unallocated Clusters
testforensic 2014 (account name)	•\home\[username]\ .cache\mozilla\firefox\sellmnkv.default\Cache	•\home\[username]\ .cache\ google-chrome\Default\
test123456 789 (password)	none	none
1.doc (test file)	none	none
This is Microsoft word. (text in the 1.doc)	none	none

Access-VM

In these virtual machines, UMF-Access, and UGC-Access, we use different browser to log in Amazon Cloud Storage and only online open the test files which are uploaded previously. Then we log out and close the browser, and shut down the system. We find the remnants by Guidance EnCase v7.04. We find the keyword Amazon in different directories. In MF and GC cache, we find it on \home\[username]\.cache\mozilla\firefox\sellmnkv.default\ Cache in UMF-Access and \home\[username]\.cache\google-chrome\Default\ in UGC-Access. We also find it on System Folder \usr\lib\ and \usr\share\. It also can be found on the \Unallocated Clusters. About account name, we find it on \home\[username]\.cache\mozilla\firefox\sellmnkv.default\

Cache in UMF-Access and on \home\[username]\.config\google-chrome\Default\ in UGC-Access. We can't find the password because it was not stored on the files of disk. We open the test files online and have no data remnants on the browser's cache. Table 2 shows the remnants of Access-VMs.

Upload-VM

We use upload virtual machines to upload test files. These upload virtual machines are UMF-Upload, and UGC-Upload. The test files are uploaded to Amazon Cloud Storage. Then we delete test files from the virtual machines. After we open the test files from Amazon Cloud Storage, we close the browser, then shuts down the system. We find the keyword Amazon, test account name, and password in the same directories as Access-VM. About test files, we find data remnants on Trash \home\[username]\.local\share\Trash and System log area \Journal Area in UMF-Upload and UGC-Upload. It proves the files have been deleted. About text in files, we can find data remnants on \Unallocated Clusters in UMF-Upload and UGC-Upload. It also proves the text has been deleted.

Download-VM

We use download virtual machines to download test files. These download virtual machines are UMF-Download, and UGC-Download. The test files are downloaded from Amazon Cloud Storage. We log out from Amazon Cloud Storage. After we open test files from the virtual machines, we close test files immediately. We find data remnants of the keyword Amazon, test account name, and password in the same directories as Access-VM. About test files, we find data remnants on \home\[username]\.cache\mozilla\firefox\sellmnkv.default\Cache, and \Unallocated Clusters in UMF-Download and \home\[username]\.config\google-chrome\Default\ and \Unallocated Clusters in UGC-Download. About text in the files, we can find data remnants on \home\[username]\download\ in UMF-Download and on \home\[username]\.cache\google-chrome\Default\ and \home\[username]\download\ in UGC-Download.

BleachBit-VM

We do the same actions as Download-VM. Then we run BleachBit to delete browser data remnants such as password, cookies, cache, history, etc. We also delete the history of the Windows Explorer such as most recently used files list, image cache, Recycle Bin, Scrapbook, etc. We find data remnants of the keyword Amazon, and test account name on \home\[username]\.cache\mozilla\firefox\sellmnkv.default\Cache in UMF-BleachBit, and \home\[username]\.cache\google-chrome\Default\Cache\ in UGC-BleachBit. The keyword Amazon can also find on \usr\share\ and \Unallocated Clusters in UMF-BleachBit and UGC-BleachBit. About test files, we find data remnants on system log area \Journal Area and \Unallocated Clusters in UMF-BleachBit and UGC-BleachBit. We also find data remnants on \home\[username]\.local\share\Trash in UMF-BleachBit and on \home\[username]\.config\google-chrome\Default\ in UGC-BleachBit. About text in the files, we can find data remnants on \home\[username]\.local\share\Trash\files\ in UMF-BleachBit and on \Unallocated Clusters in UGC-BleachBit.

Table 3: The remnants of BleachBit-VM

Keyword	Firefox	Google Chrome
Amazon	•\home\[username]\.cache\mozilla\firefox\sellmnkv.default\Cache •\usr\share\ •\Unallocated Clusters	•\home\[username]\.cache\ google-chrome\Default\ •\usr\share\ •\Unallocated Clusters
testforensic 2014 (account name)	•\home\[username]\.cache\mozilla\firefox\sellmnkv.default\Cache	•\home\[username]\.cache\ google-chrome\Default\
test123456789 (password)	none	none
1.doc (test file)	•\home\[username]\.local\share\Trash •\Journal Area •\Unallocated Clusters	•\home\[username]\.config\google-chrome\Default\ •\Journal Area •\Unallocated Clusters
This is Microsoft word. (text in the 1.doc)	•\home\[username]\.local\share\Trash\files\1.doc	•\Unallocated Clusters

Based on the above discussion, the key evidences always appear in the trash, system logs, and unallocated space. In the Upload-VM, after the action of deleting file we can find evidences on \home\[username]\.local\share\Trash and \Journal Area. We know it's a basic deletion action. In the BleachBit-VM, we can find the evidences in the same location as Upload-VM and we also find it on \Unallocated Clusters. It means we do the action of BleachBit. Table 3 shows the remnants of BleachBit-VM.

5. Conclusions

With the increasing use of cloud computing, the continued development of the digital forensic discipline is more important than ever. In our study, we found that an examiner can examine common file locations to locate software and files. We found that an Amazon Cloud Drive username can be determined from browser history when web access has been undertaken with Mozilla Firefox and Google Chrome.

The remnants of cloud activity can be found on local machines. It could be valuable for the forensic examiners. We found the remnants in local folders. The username, the cache files, and log activity which helps in recovering the deleted files and data. We identify the locations of data and files to determine user details and cloud storage information relating to use of Amazon Cloud Drive in our research.

References

[1] Mell, P & Grance, T. The Nist Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145. 2011.

[2] Ameer Pichan, Mihai Lazarescu, Sie Teng Soh. Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation 2015;13:38-57.

[3] Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 2015;42(21):7905–7916.

[4] IDC: Worldwide Public Cloud Services Spending Forecast. 2016; https://www.idc.com/getdoc.jsp?containerId=prUS40960516 (Access on May 20, 2016)

[5] Zawaod S, Hasan R. Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Distributed, Parallel, and Cluster Computing. 2013;arXiv:1302.6312.

[6] RightScale 2016 State of the Cloud Report. http://www.mcit.gov.eg/Upcont/Documents/Reports%20and%20Documents_1252016000_RightScale-2016-State-of-the-Cloud-Report.pdf (Access on May 20, 2016).

[7] Biggs, S & Vidalis, S. Cloud Computing: The Impact on Digital Forensic Investigations. Proceedings of IEEE International Conference for Internet Technology and Secured Transactions. 2009;1–6.

[8] Guo, H, Shang, T & Jin, B. Forensic Investigations in Cloud Environments. IEEE International Conference on Computer Science and Information Processing. 2012;248-251.

[9] Taylor, M, Haggerty, J, Gresty, D & Lamb, D. Forensic Investigation of Cloud Computing Systems. Network Security. 2011;3:4-10.

[10] Lumley, RA. Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business. The Vice President for Research, and the School of Engineering and Applied Science of The George Washington University. 2010;21.

[11] Reilly, D, Wren, C & Berry. Cloud Computing: Pros and Cons for Computer Forensic Investigations. International Journal of Multimedia and Image Processing. 2011;1:26-34.

[12] McClain, F. Dropbox Forensics. 2011; https://articles.forensicfocus.com/2011/07/24/dropbox-forensics/ (Access on May 20, 2016).

[13] Chung, H, Park, J, Lee, S & Kang, C (2012), Digital Forensic Investigation of Cloud Storage Services, Digital Investigation. 2012; 9(2): 81–95.

[14] Hale, Jason. Amazon Cloud Drive Forensic Analysis. Digital Investigation. 2013;10(3): 259- 265.

[15] D. Quick and K.-K. R. Choo, Dropbox analysis: Data remnants on user machines. Digital Investigation. 2013;10(1): 3-18.

[16] Darren Quick, Kim-Kwang Raymond Choo, "Google Drive: forensic analysis of cloud storage data remnants," Journal of Network and Computer Applications. 2014;40:179-193.

[17] Darren Quick, Kim-Kwang Raymond Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," Future Generation Computer Systems. 2013;29(6):1378-1394.

[18] S. Mehreen, B. Aslam. Windows 8 Cloud Storage Analysis: Dropbox Forensics. International Bhurban Conference on Applied Sciences & Technology. 2015;312-317

[19] Zhu, M. Mobile Cloud Computing: Implications to Smartphone Forensic Procedures and Methodologies. AUT University, 2011.

[20] Reese, G. Cloud Forensics Using Ebs Boot Volumes, Oreilly.com, 2010.

[21] Clark, P. Digital Forensics Tool Testing–Image Metadata in the Cloud, Department of Computer Science and Media Technology, Gjøvik University College, 2011.